

BALANCED SYMMETRIC FUNCTIONS OVER $GF(p)$ THOMAS W. CUSICK¹, YUAN LI², PANTELIMON STĂNICĂ^{3*}

ABSTRACT. Under mild conditions on n, p , we give a lower bound on the number of n -variable balanced symmetric polynomials over finite fields $GF(p)$, where p is a prime number. The existence of nonlinear balanced symmetric polynomials is an immediate corollary of this bound. Furthermore, we conjecture that $X(2^t, 2^{t+1}l - 1)$ are the only nonlinear balanced elementary symmetric polynomials over $GF(2)$, where $X(d, n) = \sum_{i_1 < i_2 < \dots < i_d} x_{i_1} x_{i_2} \dots x_{i_d}$, and we prove various results in support of this conjecture.

1. INTRODUCTION

Since symmetry guarantees that all of the input bits have equal status in a very strong sense, symmetric Boolean functions display some interesting properties. A lot of research about symmetry in characteristic 2 has been previously done in [1, 3, 5, 6, 7, 9, 10, 18, 19, 20, 21, 24, 26]. On the other hand, it is natural to extend various cryptographic ideas from $GF(2)$ to other finite fields of characteristic > 2 , $GF(p)$ or $GF(p^n)$, p being a prime number. For example, [16] and [25] studied the correlation immune and resilient functions on $GF(p)$. Also, [8] and [14] investigated the generalized bent functions on $GF(p^n)$. In [23], Li and Cusick first introduced the strict avalanche criterion over $GF(p)$. In [24], they generalized most results of [7] and determined all the linear structures of symmetric functions over $GF(p)$.

Balancedness is a desirable requirement of functions which will be used in cryptography. In this paper, by an enumerating method, we give a lower bound for the number of balanced symmetric polynomials over $GF(p)$, and as an immediate consequence, we show the existence of nonlinear balanced symmetric polynomials. We did not find (even conjecturally) any simple characterization of the algebraic normal form of nonlinear balanced symmetric polynomials even for $p = 2$. However, we do make substantial progress in the binary case if the polynomial is elementary symmetric (Section 5 below). We prove some results toward the conjecture that the polynomials $X(2^t, 2^{t+1}l - 1)$ are the *only* nonlinear balanced elementary symmetric polynomials, where $X(d, n) = \sum_{i_1 < i_2 < \dots < i_d} x_{i_1} x_{i_2} \dots x_{i_d}$.

Date: February 2, 2008.

Key words and phrases. Cryptography, finite fields, balancedness, symmetric polynomials, multinomial coefficients.

* Research supported by the Naval Postgraduate School RIP funding.

2. PRELIMINARIES

In this paper, p is a prime number. If $f: GF(p)^n \longrightarrow GF(p)$, then f can be uniquely expressed in the following form, called the *algebraic normal form* (ANF):

$$f(x_1, x_2, \dots, x_n) = \sum_{k_1, k_2, \dots, k_n=0}^{p-1} a_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n},$$

where each coefficient $a_{k_1 k_2 \dots k_n}$ is a constant in $GF(p)$.

The function $f(x)$ is called an *affine function* if $f(x) = a_1 x_1 + \dots + a_n x_n + a_0$. If $a_0 = 0$, $f(x)$ is also called a *linear function*. We will denote by F_n the set of all functions of n variables and by L_n the set of affine ones. We will call a function *nonlinear* if it is not in L_n .

If $f(x) \in F_n$, then $f(x)$ is a *symmetric function* if for any permutation π on $\{1, 2, \dots, n\}$, we have $f(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}) = f(x_1, x_2, \dots, x_n)$. The set of permutations on $\{1, 2, \dots, n\}$ will be denoted by S_n .

We define the following equivalence relation on $GF(p)^n$: for any $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ in $GF(p)^n$, we say x and y are equivalent, and write $x \sim y$, if there exists a permutation $\pi \in S_n$ such that $(y_1, y_2, \dots, y_n) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$ (by abuse of notation we write $y = \pi(x)$). Let $\tilde{x} = \{y \mid \exists \pi \in S_n, \pi(x) = y\}$. Let $\bar{x} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$ be the representative of \tilde{x} , where $0 \leq \bar{x}_1 \leq \bar{x}_2 \leq \dots \leq \bar{x}_n \leq p-1$. Obviously, we have $\tilde{x} = \tilde{y} \iff \bar{x} = \bar{y}$.

3. ENUMERATION RESULTS

Definition 1. $f: GF(p)^n \longrightarrow GF(p)$ is *balanced* if the probability $\text{prob}(f = k) = \frac{1}{p}$ for any $k = 0, 1, \dots, p-1$.

As an immediate consequence, f is balanced if and only if $\#\{x \in GF(p)^n \mid f(x) = k\} = p^{n-1}$.

Using the equivalence relation of the previous section, we get that $f: GF(p)^n \longrightarrow GF(p)$ is symmetric if $f(x) = f(y)$ whenever $\tilde{x} = \tilde{y}$. Let $C(n, k) = \frac{n!}{k!(n-k)!}$ if $0 \leq k \leq n$ and 0 otherwise be the usual binomial coefficients. Then we have

Lemma 1. *The number of n -variable symmetric polynomials over $GF(p)$ is*

$$p^{C(p+n-1, n)}.$$

Proof. The number of different vector classes \tilde{x} is the number of solutions of the linear equation $i_0 + i_1 + \dots + i_{p-1} = n$, where i_k is the number of times k appears in \bar{x} . We know that the number of solutions to the previous linear diophantine equation is the same as the number of n -combinations of a set with p elements, that is $C(p+n-1, n)$ (see [4, p. 69]). Since a symmetric function $f(x)$ has the same value for any element of \tilde{x} , the lemma is proved. \square

Lemma 2. *We have $\prod_{k=0}^{p-1} C((k+1)a, a) = \frac{(pa)!}{(a!)^p}$.*

Proof. It is a straightforward computation

$$\prod_{k=0}^{p-1} C((k+1)a, a) = \frac{a!}{a!} \frac{(2a)!}{a!a!} \frac{(3a)!}{a!(2a)!} \dots \frac{(pa)!}{a!((p-1)a)!} = \frac{(pa)!}{(a!)^p}.$$

\square

Lemma 3. *The number of n -variable balanced polynomials over $GF(p)$ is*

$$\frac{(p^n)!}{(p^{n-1}!)^p}.$$

Proof. The number we are looking for is

$$C(p^n, p^{n-1})C(p^n - p^{n-1}, p^{n-1}) \cdots C(p^n - (p-1)p^{n-1}, p^{n-1}) = \frac{(p^n)!}{(p^{n-1}!)^p},$$

using Lemma 2, and the claim is proved. \square

Let $\bar{x} = (\underbrace{0, \dots, 0}_{i_0}, \underbrace{1, \dots, 1}_{i_1}, \dots, \underbrace{p-1, \dots, p-1}_{i_{p-1}})$, where $i_0 + i_1 + \cdots + i_{p-1} = n$, $0 \leq i_j \leq n$, $j = 0, 1, \dots, p-1$. The cardinality of the set \tilde{x} is the value of the multinomial coefficient $C(n, i_0, i_1, \dots, i_{p-2}) = \frac{n!}{i_0! i_1! \cdots i_{p-1}!}$. We have the following widely known multinomial expansion lemma.

Lemma 4. [4, p. 123] *We have the following formula*

$$(t_0 + t_1 + \cdots + t_{p-1})^n = \sum_{i_0 + i_1 + \cdots + i_{p-1} = n} C(n, i_0, i_1, \dots, i_{p-2}) t_0^{i_0} t_1^{i_1} \cdots t_{p-1}^{i_{p-1}}.$$

By specializing $t_0 = t_1 = \cdots = t_{p-1} = 1$, we get the following corollary.

Corollary 1. *The n -th power of p satisfies*

$$p^n = \sum_{i_0 + i_1 + \cdots + i_{p-1} = n} C(n, i_0, i_1, \dots, i_{p-2}).$$

From the proof of Lemma 1, we know that the number of terms in the sum in Corollary 1 is $C(p+n-1, n)$. It is clear now, that to get balanced symmetric polynomials amounts to partitioning the set of $C(p+n-1, n)$ many multinomial coefficients $C(n, i_0, i_1, \dots, i_{p-2})$ into p groups, the sum of each group being equal to p^{n-1} .

For a fixed solution $\{i_0, i_1, \dots, i_{p-1}\}$ of $i_0 + i_1 + \cdots + i_{p-1} = n$, there are $\frac{p!}{m_0! m_1! \cdots m_n!}$ many ways to order it, where $i_j \in \{0, 1, \dots, n\}$, and m_l is the number of times that l appears in $\{i_0, \dots, i_{p-1}\}$, $0 \leq l \leq n$. Hence,

$$(1) \quad m_0 + m_1 + \cdots + m_n = p, \text{ and } 0m_0 + 1m_1 + \cdots + nm_n = n.$$

Let us consider the following map:

$$F : \{\{i_0, i_1, \dots, i_{p-1}\} \mid \sum_{j=0}^{p-1} i_j = n\} \rightarrow \{(m_0, m_1, \dots, m_n) \mid \sum_{l=0}^n m_l = p, \sum_{l=0}^n l m_l = n\}$$

defined by

$$F(\{i_0, i_1, \dots, i_{p-1}\}) = (m_0, m_1, \dots, m_n),$$

where m_l is as above. It is not hard to check that F is a bijection.

Now, we will partition the set of multinomial coefficients $C(n, i_0, \dots, i_{p-2})$ using the following equivalence relation: $C(n, i_0, \dots, i_{p-2})$ and $C(n, j_0, \dots, j_{p-2})$ belong to the same class if and only if j_0, \dots, j_{p-1} is a permutation of i_0, \dots, i_{p-1} . Of course, any element in the same class has the same value. So, we can think of F as a map that assigns to each class the value $\frac{p!}{m_0! m_1! \cdots m_n!}$.

Lemma 5. *Let n, p be positive integers, with p a prime number. If $m_i < p$ for some i (and so for all i), or if $\gcd(n, p) = 1$, then p divides $\frac{p!}{m_0! m_1! \cdots m_n!}$.*

Proof. Assume $m_i < p$. By a known extension of Kummer's result that belongs to Dickson (see [13, Theorem D, p. 3860]) the power of p that divides the multinomial coefficient equals the number of carries when we add $m_0 + m_1 + \dots + m_n$ in base p , but the mentioned sum is equal to p , therefore the number of carries is 1. (One can also prove the same assertion without using Dickson's result.)

Now, assume $\gcd(n, p) = 1$. If $m_i < p$, the first part of the proof proves the claim. Assume $m_i \geq p$. Since $m_0 + m_1 + \dots + m_n = p$, we can find j such that $m_j = p$ and $m_0 = \dots = m_{j-1} = m_{j+1} = \dots = m_n = 0$. From the definition of the m_i 's we obtain that $jp = n$, which is a contradiction. \square

Remark 1. The two conditions $m_i < p$, and $\gcd(n, p) = 1$ are not equivalent (although, it is true that $\gcd(n, p) = 1$ implies $m_i < p$). For instance, by taking $m_0 = 3, m_1 = 2, m_2 = 1, m_3 = 1, m_4 = m_5 = m_6 = m_7 = 0$, we get $m_0 + m_1 + \dots + m_7 = p = 7 = n = 0m_0 + 1m_1 + \dots + 7m_7$, so $p = n$ in this case.

Since the cardinality of each multinomial coefficient class is a multiple of p , we can divide each class into p groups with an equal number of coefficients, hence, equal sum. Doing the same for each class, we finally partition all of the $C(p + n - 1, n)$ coefficients into p groups with equal sum.

For a given (m_0, m_1, \dots, m_n) , $m_0 + m_1 + \dots + m_n = p$, $0m_0 + 1m_1 + \dots + nm_n = n$, the partition number is

$$C\left(\frac{p!}{m_0!m_1!\dots m_n!}, \frac{(p-1)!}{m_0!m_1!\dots m_n!}\right) C\left(\frac{p!}{m_0!m_1!\dots m_n!} - \frac{(p-1)!}{m_0!m_1!\dots m_n!}, \frac{(p-1)!}{m_0!m_1!\dots m_n!}\right) \dots \\ C\left(\frac{p!}{m_0!m_1!\dots m_n!} - \frac{k(p-1)!}{m_0!m_1!\dots m_n!}, \frac{(p-1)!}{m_0!m_1!\dots m_n!}\right) \dots C\left(\frac{(p-1)!}{m_0!m_1!\dots m_n!}, \frac{(p-1)!}{m_0!m_1!\dots m_n!}\right).$$

By Lemma 2, this product can be written as

$$\frac{\left(\frac{p!}{m_0!\dots m_n!}\right)!}{\left(\left(\frac{(p-1)!}{m_0!\dots m_n!}\right)!\right)^p}.$$

In conclusion, we get our main result of this section.

Theorem 1. Let N be the number of n -variable balanced symmetric functions over $GF(p)$. If $m_i < p$, for all i (or $\gcd(n, p) = 1$), then

$$N \geq \prod_{\substack{\sum_{j=0}^n m_j = p \\ \sum_{j=0}^n jm_j = n}} \frac{\left(\frac{p!}{m_0!\dots m_n!}\right)!}{\left(\left(\frac{(p-1)!}{m_0!\dots m_n!}\right)!\right)^p}.$$

Next, since the linear balanced symmetric polynomials over $GF(p)$ have the form $a(x_1 + \dots + x_n) + b$, where $a \in GF(p)^*$ and $b \in GF(p)$, we get that the number of such functions is $p(p-1)$. Since $\frac{(pa)!}{(a!)^p} = \frac{a!}{a!} \frac{(2a)!}{a!a!} \frac{(3a)!}{a!(2a)!} \dots \frac{(pa)!}{a!((p-1)a)!} > 12 \dots p = p! \geq p(p-1)$, we have the next corollary.

Corollary 2. If n is not divisible by p , there exists a nonlinear n -variable balanced symmetric polynomial over $GF(p)$.

4. THE BALANCEDNESS OF ELEMENTARY SYMMETRIC POLYNOMIALS OVER $GF(2)$

In this section we consider the binary case, that is, $p = 2$. Here, we shall try to find all nonlinear balanced elementary symmetric polynomials. Throughout, $\mathbf{x} = (x_1, \dots, x_n)$ and \oplus is the addition modulo 2.

Definition 2. For integers n and d , $1 \leq d \leq n$ we define the elementary symmetric polynomial by

$$(2) \quad X(d, n) = \sum_{i_1 < i_2 < \dots < i_d} x_{i_1} x_{i_2} \cdots x_{i_d}.$$

By abuse of notation, we let $X(d, n)(j)$ be the value of $X(d, n)$ when $wt(\mathbf{x}) = j$. Since $X(d, n)(j) \equiv C(j, d) \pmod{2}$, we get

$$X(d, n)(j) = \frac{1 - (-1)^{C(j, d)}}{2}.$$

Because there are $C(n, j)$ many vectors with weight j , we have the following theorems.

Theorem 2. *The elementary symmetric polynomial $X(d, n)$ is balanced if and only if*

$$\sum_{0 \leq j \leq n} C(n, j)(-1)^{C(j, d)} = 0.$$

Theorem 3. *If $X(d, n)$ is balanced, then $d \leq \lceil n/2 \rceil$.*

Proof. If n is even and $d \geq \frac{n}{2} + 1$, then

$$\sum_{C(j, d) \equiv 0 \pmod{2}} C(n, j) > C(n, 0) + C(n, 1) + \cdots + C(n, n/2) > 2^{n-1}.$$

If n is odd and $k \geq \frac{n+1}{2} + 1$, then

$$\sum_{C(j, d) \equiv 0 \pmod{2}} C(n, j) > C(n, 0) + C(n, 1) + \cdots + C(n, (n+1)/2) > 2^{n-1}.$$

In both cases, we have

$$\begin{aligned} & \sum_{0 \leq j \leq n} C(n, j)(-1)^{C(j, d)} \\ &= \sum_{C(j, d) \equiv 0 \pmod{2}} C(n, j) - \sum_{C(j, d) \equiv 1 \pmod{2}} C(n, j) \\ &= \sum_{C(j, d) \equiv 0 \pmod{2}} C(n, j) - \left(2^n - \sum_{C(j, d) \equiv 0 \pmod{2}} C(n, j) \right) \\ &= 2 \left(\sum_{C(j, d) \equiv 0 \pmod{2}} C(n, j) - 2^{n-1} \right) > 0, \end{aligned}$$

contradicting Theorem 2. □

Therefore, we see from Theorem 2 that the existence of balanced elementary symmetric polynomials is related to the problem of bisecting binomial coefficients (defined below). In [6], two of us found some computational results about such bisections, which results we shall describe below. (We mention here that the authors of [20] found the number of solutions but without the explicit solutions.) It was suspected that the existence of nontrivial binomial coefficient bisections (as in [6]) may cause difficulties in the study of the existence of balanced symmetric polynomials, but we conjecture that this is not true for the elementary symmetric case.

We begin with

Definition 3. [6] If $\sum_{i=0}^n \delta_i C(n, i) = 0$, $\delta_i \in \{-1, 1\}$, $i = 0, 1, \dots, n$, we call $(\delta_0, \dots, \delta_n)$ a solution of the equation

$$(3) \quad \sum_{i=0}^n x_i C(n, i) = 0, \quad x_i \in \{-1, 1\}.$$

In fact, whenever we get a solution of (3), we get a bisection of binomial coefficients, that is, we find A, B such that $A \cup B = \{0, 1, \dots, n\}$, $A \cap B = \emptyset$, $\sum_{i \in A} C(n, i) = \sum_{i \in B} C(n, i) = 2^{n-1}$.

Obviously, if n is even, then $\pm(1, -1, 1, -1, \dots, 1)$ are two solutions of (3). If n is odd, then $(\delta_0, \dots, \delta_{\frac{n-1}{2}}, -\delta_{\frac{n-1}{2}-1}, \dots, -\delta_0)$ are $2^{\frac{n+1}{2}}$ solutions of (3). We call these trivial solutions.

Mitchell [19] mentioned the nontrivial solutions for $n = 8, 13$. In [6], with a C++ program, we found all solutions of (3) when $n \leq 28$. Nontrivial solutions exist if and only if $n = 8, 13, 14, 20, 24, 26$. So, here we ask the question of determining necessary and sufficient conditions on the parameter n such that there exist nonlinear balanced symmetric polynomials on $GF(2)^n$.

First, we recall a known result that enables one to find residues of binomial coefficients modulo a prime p .

Lemma 6 (Lucas' Theorem). *Let $n = a_m p^m + a_{m-1} p^{m-1} + \dots + a_1 p + a_0$ with $0 \leq a_i \leq p-1$ and $k = b_m p^m + b_{m-1} p^{m-1} + \dots + b_1 p + b_0$ with $0 \leq b_i \leq p-1$, then $C(n, k) \equiv C(a_m, b_m) \cdots C(a_1, b_1) \pmod{p}$*

The next lemma can be derived from [1]. However, here we give a direct proof.

Lemma 7. *For any integer $d \geq 2$, the sequence $\{(-1)^{C(j,d)}\}_{j=0}^\infty$ is periodic of least period $2^{\lceil \log_2 d \rceil + 1}$.*

Proof. First, recall that d has at most $\lceil \log_2 d \rceil + 1$ bits. For $0 \leq i \leq 2^{\lceil \log_2 d \rceil + 1} - 1$, according to Lemma 6, we have $C(i + 2^{\lceil \log_2 d \rceil + 1}, d) \equiv C(1, 0)C(i, d) \equiv C(i, d) \pmod{2}$, so the least period is a divisor of $2^{\lceil \log_2 d \rceil + 1}$. On the other hand, $1 = C(d, d)$ and $C(d + 2^{\lceil \log_2 d \rceil}, d) \equiv C(1, 0)C(0, 1) \cdots \equiv 0 \pmod{2}$, which implies that $2^{\lceil \log_2 d \rceil}$ cannot be a period. The lemma is proved. \square

With the help of Lemma 7, we get the following computational results. The list could easily be extended.

Lemma 8. *We have*

$$\begin{aligned} \left\{ \frac{1 - (-1)^{C(j,2)}}{2} \right\}_{j=0}^\infty &= \overline{0011} \\ \left\{ \frac{1 - (-1)^{C(j,3)}}{2} \right\}_{j=0}^\infty &= \overline{0001} \\ \left\{ \frac{1 - (-1)^{C(j,4)}}{2} \right\}_{j=0}^\infty &= \overline{00001111} \\ \left\{ \frac{1 - (-1)^{C(j,5)}}{2} \right\}_{j=0}^\infty &= \overline{00000101} \\ \left\{ \frac{1 - (-1)^{C(j,6)}}{2} \right\}_{j=0}^\infty &= \overline{00000011} \\ \left\{ \frac{1 - (-1)^{C(j,7)}}{2} \right\}_{j=0}^\infty &= \overline{00000001} \\ \left\{ \frac{1 - (-1)^{C(j,8)}}{2} \right\}_{j=0}^\infty &= \overline{0000000011111111} \\ \left\{ \frac{1 - (-1)^{C(j,9)}}{2} \right\}_{j=0}^\infty &= \overline{0000000001010101} \end{aligned}$$

$$\begin{aligned}
\left\{ \frac{1-(-1)^{C(j,10)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000110011} \\
\left\{ \frac{1-(-1)^{C(j,11)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000010001} \\
\left\{ \frac{1-(-1)^{C(j,12)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000001111} \\
\left\{ \frac{1-(-1)^{C(j,13)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000000101} \\
\left\{ \frac{1-(-1)^{C(j,14)}}{2} \right\}_{j=0}^{\infty} &= \overline{0000000000000011}
\end{aligned}$$

Theorem 4. *If t, l are positive integers, then $X(2^t, 2^{t+1}l - 1)$ is balanced.*

Proof. First, $C(j, 2^t) = 0$ when $0 \leq j \leq 2^t - 1$. By Lucas' Theorem, we have

$$C(j, 2^t) \equiv 1 \pmod{2} \text{ when } 2^t \leq j \leq 2^{t+1} - 1.$$

By Lemma 7, the period of $\{(-1)^{C(j, 2^t)}\}_{j=0}^{\infty}$ is 2^{t+1} . Hence, we get the sequence $\{(-1)^{C(j, 2^t)}\}_{j=0}^{2^{t+1}l-1}$ by repeating $\underbrace{++ \cdots +}_{2^t} \underbrace{-- \cdots -}_{2^t}$ exactly l times. Obviously

$\{(-1)^{C(j, 2^t)}\}_{j=0}^{2^{t+1}l-1}$ is a (trivial) solution of the equation $\sum_{i=0}^n x_i C(n, i) = 0$ when $n = 2^{t+1}l - 1$. Using Theorem 2 we obtain our result. \square

We conjecture that the functions in Theorem 4 are the only balanced ones.

Conjecture 1. *There are no nonlinear balanced elementary symmetric polynomials except for $X(2^t, 2^{t+1}l - 1)$, where t and l are any positive integers.*

5. RESULTS CONCERNING CONJECTURE 1

The remainder of the paper will be devoted to the study of Conjecture 1. A Boolean function $f(\mathbf{x})$ in n variables is said to satisfy the *Strict Avalanche Criterion* ("is SAC" for short) if changing any one of the n bits in the input \mathbf{x} results in the output of the function being changed for exactly half of the 2^{n-1} vectors \mathbf{x} with the changed input bit. The SAC concept is relevant for our work because of

Lemma 9. *The function $f(\mathbf{x}) = X(d, n)$ is SAC if and only if $X(d-1, n-1)$ is balanced.*

Proof. By definition, f is SAC if and only if

$$f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a}) \text{ is balanced for all } \mathbf{a} \in GF(2)^n, \text{ with } wt(\mathbf{a}) = 1.$$

We have $f(\mathbf{x}) \oplus f(\mathbf{x} \oplus (0, \dots, 0, 1)) = X(d-1, n-1)$, so the lemma is proved. \square

We previously mentioned that any symmetric function is completely determined by the weight of its input, that is, $f(\mathbf{x}) = v_f(wt(\mathbf{x}))$. Moreover, recall the usual algebraic normal form (ANF) of a Boolean function f in n variables

$$f(x_1, \dots, x_n) = \bigoplus_{i=0}^n \lambda_f(i) \bigoplus_{\mathbf{u}, wt(\mathbf{u})=i} \prod_{j=1}^n x_j^{u_j},$$

where $v_f(i) = \bigoplus_{j \preceq i} \lambda_f(j)$, and $\lambda_f(i) = \bigoplus_{j \preceq i} v_f(j)$, over $GF(2)$ ($j \preceq i$ means that the binary expansion of j is less than the binary expansion of i , in lexicographical order) (see [1, Propositions 1 and 2, p. 2792]).

The ANF of a symmetric function becomes

$$(4) \quad f(x_1, \dots, x_n) = \bigoplus_{d=0}^n \lambda_f(d) X(d, n),$$

in our notations. Further, when f is an elementary symmetric function, then $\lambda_f(d) = 1$ is the only nonzero coefficient in the representation (4). Moreover,

$$(5) \quad v_f(i) = \bigoplus_{j \preceq i} \lambda_f(j) = \begin{cases} \lambda_f(d), & \text{if } d \preceq i \\ 0, & \text{otherwise.} \end{cases}$$

We need the following further lemmas. We define the well known Walsh transform $W_f(\mathbf{w})$ by

$$W_f(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{w}}.$$

Lemma 10. *A Boolean function f in n variables is SAC if and only if for every vector \mathbf{u} with $wt(\mathbf{u}) = 1$ and every vector \mathbf{v} , we have*

$$\sum_{\mathbf{w} \preceq \bar{\mathbf{u}}} W_f(\mathbf{w} \oplus \mathbf{v})^2 = 2^{wt(\bar{\mathbf{u}}) + n}.$$

Proof. This is a special case of Proposition 1 of Carlet [2, p. 35]. \square

Lemma 11. *If $f(\mathbf{x})$ in n variables is SAC, then*

$$(6) \quad \sum_{\mathbf{w}: w_n=0} W_f(\mathbf{w})^2 = \sum_{\mathbf{w}: w_n=1} W_f(\mathbf{w})^2 = 2^{2n-1}.$$

Proof. We use Lemma 10 with $\mathbf{v} = \mathbf{0}$ and $\mathbf{u} = (0, \dots, 0, 1)$. It follows that $wt(\bar{\mathbf{u}}) = n-1$, so the first sum in (6) equals 2^{2n-1} . The two sums add up to 2^{2n} by Parseval's Theorem, so the second sum is also 2^{2n-1} . \square

Lemma 12. *If $f(\mathbf{x}) = X(d, n)$ is SAC and d is odd, then*

$$(7) \quad W_f(\mathbf{0}) = 2^n - 2 \, wt(f) \quad \text{and} \quad W_f(\mathbf{1}) = 2 \, wt(f).$$

Proof. The first equation in (7) is clear for any f , whether or not d is odd.

For the second equation, we observe that by (5) our hypotheses imply that $v_f(k) = 0$ for all even k . Since

$$W_f(\mathbf{0}) = \sum_{k=0}^n (-1)^{v_f(k)} C(n, k) \quad \text{and} \quad W_f(\mathbf{1}) = \sum_{k=0}^n (-1)^{v_f(k)+k} C(n, k),$$

a computation gives

$$W_f(\mathbf{0}) + W_f(\mathbf{1}) = 2^n.$$

Now the second equation in (7) follows from the first one. \square

We define

$$(8) \quad \begin{aligned} A &= 0, 0, 1, 1; \quad \bar{A} = 1, 1, 0, 0; \quad B = 0, 1, 0, 1; \quad \bar{B} = 1, 0, 1, 0; \\ C &= 0, 1, 1, 0; \quad \bar{C} = 1, 0, 0, 1; \quad D = 0, 0, 0, 0; \quad \bar{D} = 1, 1, 1, 1. \end{aligned}$$

The next two lemmas are used in the proof of our Theorem 5.

Lemma 13. (Folklore Lemma [22, Lemma 3.7.2]) *Any affine function f on n variables, $n \geq 2$, is a linear string of length 2^n made up of 4-bit blocks $I_1, \dots, I_{2^{n-2}}$ given as follows:*

1. The first block I_1 is one of $A, B, C, D, \bar{A}, \bar{B}, \bar{C}$ or \bar{D} .
2. The second block I_2 is I_1 or \bar{I}_1 .
3. The next two blocks I_3, I_4 are I_1, I_2 or \bar{I}_1, \bar{I}_2 .

.....
 $n - 1$. The 2^{n-3} blocks $I_{2^{n-3}+1}, \dots, I_{2^{n-2}}$ are $I_1, \dots, I_{2^{n-3}}$ or $\bar{I}_1, \dots, \bar{I}_{2^{n-3}}$.

Lemma 14. We have $\sum_{\mathbf{x}, wt(\mathbf{x}) \text{ even}} (-1)^{\mathbf{x} \cdot \mathbf{w}} = 0$ for all $\mathbf{w} \neq \mathbf{0}$ or $\mathbf{1}$.

Proof. Let $E(\mathbf{w})$ denote the 2^{n-1} -vector of bits $\mathbf{x} \cdot \mathbf{w} \pmod{2}$, where \mathbf{x} runs through the n -vectors \mathbf{x} of even weight in lexicographical order. Thus $E(\mathbf{w})$ lists the exponents in the sum in the lemma. Consider the 2^{n-1} by n array of the vectors \mathbf{x} with even weight, taken in lexicographical order. By the Folklore Lemma, each column in this array is a 2^{n-1} -vector which gives the truth table of a nonconstant linear function in $n - 1$ variables. In fact, taking the columns left to right, the functions are simply $x_1, x_2, \dots, x_{n-1}, x_1 \oplus x_2 \oplus \dots \oplus x_{n-1}$. The vector sum of any subset of at least one and at most $n - 1$ of the n columns (corresponding to $\mathbf{w} \neq \mathbf{0}$ or $\mathbf{1}$) is thus the truth table of a nonconstant linear function and so it is balanced. Each vector $E(\mathbf{w})$ is one of these vector sums, so the sum in the lemma is 0. \square

Remark 2. The sum in Lemma 13 is the sum of the Krawtchouk polynomials [17, pp. 130 and 150–153] (variable $y = wt(\mathbf{w})$)

$$P_k(y, n) = \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}} = \sum_{j=0}^k (-1)^j C(y, j) C(n - y, k - j)$$

of even degree k in y .

Theorem 5. If $f(\mathbf{x}) = X(d, n)$ has odd degree d , then $W_f(\mathbf{w}) = -W_f(\bar{\mathbf{w}})$ for all $\mathbf{w} \neq \mathbf{0}$ or $\mathbf{1}$.

Proof. Let f be an elementary symmetric function of degree k , that is $f = X(d, n)$. We compute the Walsh transform

$$\begin{aligned}
 W_f(\bar{\mathbf{w}}) &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{x} \cdot \bar{\mathbf{w}}} \\
 &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{x} \cdot (\mathbf{1} + \mathbf{w})} \\
 &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + wt(\mathbf{x}) + \mathbf{x} \cdot \mathbf{w}} \\
 (9) \quad &= \sum_{k=0}^n \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{f(\mathbf{x}) + wt(\mathbf{x}) + \mathbf{x} \cdot \mathbf{w}} \\
 &= \sum_{k=0}^n (-1)^{v_f(k) + k} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}}.
 \end{aligned}$$

Next, we use (5). Since d is odd, then any integer i with $d \preceq i$ has to be odd, as well. It follows that $v_f(k) = 0$, for any even integer k . Thus, (9) becomes

$$\begin{aligned}
W_f(\bar{\mathbf{w}}) &= \sum_{k=0}^n (-1)^{v_f(k)+k} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}} \\
&= \sum_{k=0, \text{ even}}^n (-1)^{v_f(k)} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}} \\
&\quad - \sum_{k=0, \text{ odd}}^n (-1)^{v_f(k)} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}} \\
&= \sum_{\mathbf{x}, wt(\mathbf{x})=\text{even}} (-1)^{\mathbf{x} \cdot \mathbf{w}} - \sum_{k=0, \text{ odd}}^n (-1)^{v_f(k)} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}}.
\end{aligned}$$

Since

$$\begin{aligned}
W_f(\mathbf{w}) &= \sum_{k=0, \text{ even}}^n (-1)^{v_f(k)} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}} \\
&\quad + \sum_{k=0, \text{ odd}}^n (-1)^{v_f(k)} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}} \\
&= \sum_{\mathbf{x}, wt(\mathbf{x})=\text{even}} (-1)^{\mathbf{x} \cdot \mathbf{w}} + \sum_{k=0, \text{ odd}}^n (-1)^{v_f(k)} \sum_{\mathbf{x}, wt(\mathbf{x})=k} (-1)^{\mathbf{x} \cdot \mathbf{w}},
\end{aligned}$$

to prove Theorem 5 it will suffice to show that

$$\sum_{\mathbf{x}, wt(\mathbf{x})=\text{even}} (-1)^{\mathbf{x} \cdot \mathbf{w}} = 0,$$

as long as $\mathbf{w} \neq \mathbf{0}, \mathbf{1}$, and that follows from Lemma 14. \square

Theorem 6. *If $f(x) = X(d, n)$ is SAC and d is odd, then $W_f(\mathbf{0}) = W_f(\mathbf{1})$.*

Proof. By Theorem 5, all of the terms except $W_f(\mathbf{0})^2$ and $W_f(\mathbf{1})^2$ in the two sums in (6) cancel out (for all other \mathbf{w} , $W_f(\mathbf{w})$ is in one sum and $W_f(\bar{\mathbf{w}})$ is in the other sum). By Lemma 12, both square roots are positive and we get Theorem 6. \square

Corollary 3. *If d is odd and $f(\mathbf{x}) = X(d, n)$ is SAC, then $wt(f) = 2^{n-2}$.*

Now we determine when $X(d, n)$ is SAC. To deal with the case when d is an even integer, by Lemma 9, it is enough to show:

Lemma 15. *If $d > 1$ is odd, then $X(d, n)$ is not balanced.*

Proof. Formula (5) shows that when $f = X(d, n)$ we have $v_f(i) = 1$ if and only if $d \preceq i$. Thus we have

$$(10) \quad wt(X(d, n)) = \sum_{d \preceq i, i \leq n} C(n, i) \leq \sum_{i \text{ odd}} C(n, i) = 2^{n-1},$$

where the inequality holds because $d \preceq i$ and d odd implies i is odd. If $d > 1$, then $d \preceq i$ cannot hold for all odd $i \leq n$ (in particular, $d \not\preceq d-2$), so the inequality in (10) is strict. Therefore, $X(d, n)$ is not balanced. \square

Lemma 16. *Suppose $d > 1$ is odd. If*

$$(11) \quad d = 2^t + 1 \text{ and } n = 2^{t+1}\ell \text{ for some positive integers } t, \ell,$$

then $wt(X(d, n)) = 2^{n-2}$.

Proof. First we observe

$$(12) \quad wt(X(d, n)) = \sum_{d \preceq i, i \leq n} C(n, i)$$

because of (5), which shows that when $f = X(d, n)$ we have $v_f(i) = 1$ if and only if $d \preceq i$. By (12), we need to show that

$$(13) \quad wt(X(d, n)) = \sum_{d \preceq i, i \leq n} C(n, i) = 2^{n-2}$$

if and only if (11) holds. If (11) holds, the sum in (13) is

$$\begin{aligned} & \sum_{2^t+1 \preceq i, i \leq 2^{t+1}\ell} C(2^{t+1}\ell, i) = \\ & \sum_{2^t+1 \preceq i, i \leq 2^{t+1}\ell} (C(2^{t+1}\ell - 1, i) + C(2^{t+1}\ell - 1, i - 1)) = \\ & \sum_{2^t \preceq i-1, i-1 \leq 2^{t+1}\ell-1} (C(2^{t+1}\ell - 1, i) + C(2^{t+1}\ell - 1, i - 1)) = \\ & \sum_{2^t \preceq j, j \leq 2^{t+1}\ell-1} C(2^{t+1}\ell - 1, j) = 2^{n-2}, \end{aligned}$$

(note i is never even in the first three sums, since then $2^t + 1 \preceq i$ is false; this justifies the second last equality, since in the last sum j runs through disjoint pairs of consecutive integers) where the last sum is $wt(X(2^t, 2^{t+1}\ell - 1))$ by (12) and so is 2^{n-2} by Theorem 4. Thus we have proved that (11) implies (13). \square

We would like to prove the converse of the previous lemma. The following work moves toward that goal, but does not achieve it. Next, we prove five lemmas, which establish many cases of the converse of Lemma 16.

Lemma 17. *Let $n = 2^{t+1}\ell$ for some positive integers t, ℓ . If j is odd and $2^t + 1 < j < 2^{t+1} + 1$, then $wt(X(j, n)) < 2^{n-2}$.*

Proof. The argument of the previous lemma shows that if (11) and (13) hold for some given t and ℓ , then the set

$$S(t, \ell) = \{i : 2^t + 1 \preceq i, i \leq 2^{t+1}\ell = n\}$$

gives a set of binomial coefficients $\{C(n, i) : i \in S(t, \ell)\}$ whose sum is 2^{n-2} . (It is easy to see that $S(t, \ell)$ has $n/4$ elements, but we do not need this fact.) Now suppose that (13) holds for $n = 2^{t+1}\ell$ and for some odd $d = j$, say, satisfying $2^t + 1 < j < 2^{t+1} + 1$. Then $wt(j) > 2$, so the set

$$T(j, n) = \{i : j \preceq i, i \leq 2^{t+1}\ell = n\}$$

is a proper subset of $S(t, \ell)$. Therefore the sum of the binomial coefficients in $\{C(n, i) : i \in T(j, n)\}$ is $< 2^{n-2}$, contradicting our assumption that (13) holds with $d = j$. \square

Since we refer to it often, we include here for completeness an equation given by Canteaut and Videau in [1] (these sums are called *lacunary sums of binomial coefficients*, see [15]). Results like this concerning the binomial coefficients are very old. Some proofs and references are given in [12].

Lemma 18. *For positive integers i, n, p , we have*
(14)

$$A_n^{2^p}(i) = \sum_{\substack{0 \leq j \leq n \\ j \equiv i \pmod{2^p}}} C(n, j) = 2^{n-p} + 2^{1-p} \sum_{j=1}^{2^{p-1}-1} \left(2 \cos \left(\frac{j\pi}{2^p} \right) \right)^n \cos \left(\frac{j(n-2i)\pi}{2^p} \right)$$

Lemma 19. *Let t, r be positive integers. Suppose that $a_1 > a_3 \geq a_5 \geq \dots \geq a_J$, with $J = 2K + 1$, are nonnegative integers. Define the sum*

$$\mathbf{T} = \sum_{1 \leq j \leq J} a_j \sin \left(\frac{jr\pi}{2^{t+1}} \right).$$

If $\mathbf{T} = 0$, then $r \equiv 0 \pmod{2^{t+1}}$.

Proof. Write $b_k = a_j$, for $j = 2k + 1$. For convenience, let $\alpha = \frac{r\pi}{2^{t+1}}$. Then, using Abel's summation formula, \mathbf{T} becomes

$$\begin{aligned} \mathbf{T} &= \sum_{k=0}^K b_k \sin((2k+1)\alpha) \\ &= \sum_{m=0}^{K-1} (b_m - b_{m+1}) \sum_{k=0}^m \sin((2k+1)\alpha) + b_K \sum_{k=0}^K \sin((2k+1)\alpha). \end{aligned}$$

Note that for the first term where $m = 0$, we have $(b_0 - b_1) \sin \alpha \neq 0$, if $r \not\equiv 0 \pmod{2^{t+1}}$. Also, $(b_m - b_{m+1}) \geq 0$, and $b_K \geq 0$. The conclusion follows once we show that

$$\sin \alpha \quad \text{and} \quad \sum_{k=0}^m \sin((2k+1)\alpha)$$

have the same sign. Indeed

$$\begin{aligned} \sin \alpha \sum_{k=0}^m \sin((2k+1)\alpha) &= \frac{1}{2} \sum_{k=0}^m (\cos(2k\alpha) - \cos((2k+2)\alpha)) \\ &= \frac{1}{2} (1 - \cos((2m+2)\alpha)) \geq 0. \end{aligned}$$

The lemma is proved. □

Remark 3. *Note that \mathbf{T} above has the same sign as $\sin \alpha$.*

Because of Theorem 3, there is no loss of generality in taking $n \geq 2(d-1)$ in our next lemma.

Lemma 20. *Let r, t be positive integers, $d = 2^t + 1$, $n = 2^{t+1}$, and $r \not\equiv 0 \pmod{2^{t+1}}$. Then $wt(X(d, n+r)) \neq 2^{n+r-2}$.*

Proof. Let $d := 1 + 2^t$ be fixed. Now, using Pascal's identity, we get that $S := wt(X(d, n+r))$ satisfies

$$\begin{aligned}
S &= \sum_{d \leq i \leq n+r} C(n+r, i) = \sum_{d \leq i \leq n+r} (C(n+r-1, i) + C(n+r-1, i-1)) \\
&= \sum_{d \leq i \leq n+r-1} C(n+r-1, i) + \sum_{\substack{2^t \leq j \leq n+r-1 \\ j \text{ even}}} C(n+r-1, j) \\
&= \sum_{d \leq i \leq n+r-2} C(n+r-2, i) + \sum_{\substack{2^t \leq j \leq n+r-1 \\ j \text{ even}}} (C(n+r-1, j) + C(n+r-2, j))
\end{aligned}$$

Continuing in this manner, we obtain

$$\begin{aligned}
S &= \sum_{d \leq i \leq n+r-r} C(2^{t+1}, i) + \sum_{\substack{2^t \leq j \leq n+r-1 \\ j \text{ even}}} \sum_{k=1}^r C(n+r-k, j) \\
&= 2^{n-2} + \sum_{\substack{2^t \leq j \leq n+r-1 \\ j \text{ even}}} \sum_{k=1}^r C(n+r-k, j) \\
&= 2^{n-2} + \sum_{k=1}^r \sum_{\substack{2^t \leq j \leq n+r-1 \\ j \text{ even}}} C(n+r-k, j) \\
(15) \quad &= 2^{n-2} + \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} \sum_{\substack{j \equiv 2s+2^t \pmod{2^{t+1}} \\ 0 \leq j \leq n+r-1}} C(n+r-k, j)
\end{aligned}$$

We push further the previous identity, by computing the innermost sum. So,

$$\sum_{\substack{j \equiv 2s+2^t \pmod{2^{t+1}} \\ 0 \leq j \leq n+r-1}} C(n+r-k, j) = A_N^{2^{t+1}}(2s+2^t)$$

in the notations of Lemma 18, where $N := n+r-k$. Thus, using equation (14), we obtain

$$A_N^{2^{t+1}}(2s+2^t) = 2^{n+r-k-t-1} + 2^{-t} \sum_{a=1}^{2^t-1} \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^N \cos \frac{a(N-4s-2^{t+1})\pi}{2^{t+1}}.$$

Since

$$\cos \frac{a(N-4s-2^{t+1})\pi}{2^{t+1}} = (-1)^a \cos \frac{a(N-4s)\pi}{2^{t+1}},$$

we get

$$(16) \quad A_N^{2^{t+1}}(2s+2^t) = 2^{n+r-k-t-1} + 2^{-t} \sum_{a=1}^{2^t-1} (-1)^a \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^N \cos \frac{a(N-4s)\pi}{2^{t+1}}$$

We obtain

$$\begin{aligned}
S &= 2^{n-2} + \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} A_N^{2^{t+1}} (2s + 2^t) \\
&= 2^{n-2} + \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} 2^{n+r-k-t-1} \\
&\quad + 2^{-t} \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^N \cos \frac{a(N-4s)\pi}{2^{t+1}} \\
&= 2^{n-2} + 2^{n+r-2} \sum_{k=1}^r 2^{-k} + 2^{-t} \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^N \cos \frac{a(N-4s)\pi}{2^{t+1}} \\
&= 2^{n+r-2} + 2^{-t} \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^N \cos \frac{a(N-4s)\pi}{2^{t+1}}.
\end{aligned}$$

Therefore, to prove our assertion, we need to show that

$$\begin{aligned}
T &= \sum_{k=1}^r \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^{n+r-k} \cos \frac{a(n+r-k-4s)\pi}{2^{t+1}} \\
&= \sum_{k=1}^r \sum_{a=1}^{2^t-1} (-1)^a \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^{n+r-k} \sum_{s=0}^{2^{t-1}-1} \cos \frac{a(n+r-k-4s)\pi}{2^{t+1}} \neq 0.
\end{aligned}$$

Since

$$\frac{a(n+r-k-4s)\pi}{2^{t+1}} = a\pi + \frac{(r-k-4s)a\pi}{2^{t+1}},$$

and so,

$$\cos \left(\frac{a(n+r-k-4s)\pi}{2^{t+1}} \right) = (-1)^a \cos \left(\frac{(r-k-4s)a\pi}{2^{t+1}} \right),$$

we obtain

$$T = \sum_{k=1}^r \sum_{a=1}^{2^t-1} \left(2 \cos \frac{a\pi}{2^{t+1}} \right)^{n+r-k} \sum_{s=0}^{2^{t-1}-1} \cos \left(\frac{(r-k-4s)a\pi}{2^{t+1}} \right)$$

Formula (17.1.1) of [11] states

$$(17) \quad \sum_{s=0}^N \cos(sx + y) = \csc \frac{x}{2} \cos \left(\frac{Nx}{2} + y \right) \sin \left(\frac{(N+1)x}{2} \right).$$

Taking $A = \frac{a\pi}{2^{t+1}}$, $N = 2^{t-1} - 1$, $x = -4A$, $y = (r-k)A$ in the previous formula, we obtain

$$\begin{aligned}
\sum_{s=0}^{2^{t-1}-1} \cos((r-k-4s)A) &= \csc(-2A) \cos((2^{t-1}-1)(-2A) + (r-k)A) \sin(2^{t-1}(-2A)) \\
&= \csc(2A) \sin \left(\frac{a\pi}{2} \right) \cos \left(-\frac{a\pi}{2} + (r-k+2)A \right) \\
&= \frac{1 - (-1)^a}{2} \frac{\sin((r-k+2)A)}{\sin(2A)}.
\end{aligned}$$

Now, T becomes

$$\begin{aligned} T &= \sum_{k=1}^r \sum_{a=1}^{2^t-1} \frac{1 - (-1)^a}{2} (2 \cos A)^{n+r-k} \frac{\sin((r-k+2)A)}{\sin(2A)} \\ &= \sum_{a=1}^{2^t-1} \frac{1 - (-1)^a}{2} \frac{(2 \cos A)^{n+r}}{\sin(2A)} \sum_{k=1}^r (2 \cos A)^{-k} \sin((r-k+2)A) \end{aligned}$$

We evaluate the inside sum using formula (14.7.1) of [11]

$$\begin{aligned} \sum_{k=1}^{N-1} b^k \sin(kx + y) &= -\sin y + (1 - 2b \cos x + b^2)^{-1} \cdot \\ &\quad [\sin y + b \sin(x - y) - b^N \sin(Nx + y) \\ &\quad + b^{N+1} \sin((N-1)x + y)] \end{aligned}$$

with $N = r + 1$, $b = (2 \cos A)^{-1}$, $x = -A$, $y = (r + 2)A$. We get

$$\begin{aligned} &\sum_{k=1}^r (2 \cos A)^{-k} \sin((r-k+2)A) \\ &= -\sin((r+2)A) + b^{-2}(\sin((r+2)A) - b \sin((r+3)A) \\ &\quad - b^{r+1} \sin A + b^{r+2} \sin(2A)) \\ &= -\sin((r+2)A) + b^{-1}(2 \cos A \sin((r+2)A) - \sin((r+3)A)) \\ &\quad - b^r(2 \cos A \sin A - \sin(2A)) \\ &= -\sin((r+2)A) + 2 \cos A \sin((r+1)A) = \sin(rA). \end{aligned}$$

and so,

$$\begin{aligned} T &= \sum_{a=1}^{2^t-1} \frac{1 - (-1)^a}{2} (2 \cos A)^{n+r-1} \frac{\sin(rA)}{\sin A} \\ &= \sum_{a=1, \text{ odd}}^{2^t-1} (2 \cos A)^{n+r-1} \frac{\sin(rA)}{\sin A} \end{aligned}$$

Recall that our initial sum is

$$S = 2^{n+r-2} + 2^{-t}T,$$

so we need to prove $T \neq 0$. Observing that

$$a_j = \left(\cos \frac{j\pi}{2^{t+1}} \right)^{2^{t+1}+r-1} \cdot \frac{1}{\sin \frac{j\pi}{2^{t+1}}}$$

strictly decreases as j increases, $1 \leq j \leq 2^t - 1$, Lemma 19 shows that $T \neq 0$, thereby proving our claim. (One can prove, by a slightly more complicated method that, in fact, $T > 0$, but we did not need that.) The proof of the lemma is done. \square

Lemma 21. *If d is odd and $2^t + 1 < d \leq 2^{t+1} - 1$ for some positive integer t , then $wt(X(d, n)) \neq 2^{n-2}$ for any n of the form $n = 2^{t+1}\ell + r$, where ℓ is even and $0 \leq r < 2^{t+1} + 2^t$.*

Proof. From equation (12) we have

$$(18) \quad wt(X(2^t + 1, n)) = \sum_{k \in I(t)} \sum_{i \equiv k \pmod{2^{t+1}}, i \leq n} C(n, i)$$

where

$$\begin{aligned} I(t) &= \{k : k \text{ odd}, 2^t + 1 \leq k \leq 2^{t+1} - 1\} \\ &= \{\text{the largest } 2^{t-1} \text{ odd least positive residues} \pmod{2^{t+1}}\}. \end{aligned}$$

Let $k := 2^t + 2s + 1$, where $0 \leq s \leq 2^{t-1} - 1$, and let $A_n^{2^{t+1}}(k)$ denote the inner sum in (18). Then Lemma 18 gives (with $A = \frac{j\pi}{2^{t+1}}$)

$$\begin{aligned} (19) \quad A_n^{2^{t+1}}(k) &= 2^{n-(t+1)} + 2^{n-t} \sum_{j=1}^{2^t-1} (\cos A)^n \cos((n-2k)A) \\ &= 2^{n-(t+1)} + 2^{n-t} \sum_{j=1}^{2^t-1} (-1)^j (\cos A)^n \cos((n-2-4s)A), \end{aligned}$$

since

$$\begin{aligned} \cos((n-2k)A) &= \cos((n-2(2^t+2s+1))A) \\ &= \cos((n-4s-2)A - 2^{t+1}A) = \cos((n-4s-2)A - j\pi) \\ &= \cos((n-4s-2)A) \cos(j\pi) + \sin((n-4s-2)A) \sin(j\pi) \\ &= (-1)^j \cos((n-4s-2)A). \end{aligned}$$

If d is odd, let $J(d) \subset I(t)$ be the subset of $I(t)$, made up of the 2^{t-2} integers k that satisfy $d \preceq k \leq 2^{t+1} - 1$ (for example, if $d = 2^t + 3$, then $J(d)$ contains every other integer in $I(t)$, starting with $2^t + 3$). Let $n = 2^{t+1}\ell + r$, $0 \leq r < 2^{t+1} + 2^t$. If $r = 0$, Lemma 17 implies the result. Now, assume $1 \leq r < 2^{t+1} + 2^t$. Using (17) we obtain (recall that $A = \frac{j\pi}{2^{t+1}}$)

$$\begin{aligned} (20) \quad &\sum_{s=0}^{2^{t-1}-1} \cos(s(-4A) + (n-2)A) = \csc(-2A) \cos((2^{t-1}-1)(-2A) + (n-2)A) \sin(2^{t-1}(-2A)) \\ &= \csc(2A) \cos(-2^t A + nA) \sin\left(\frac{j\pi}{2}\right) \\ &= \csc(2A) \left(\cos\left(\frac{j\pi}{2}\right) \cos(nA) + \sin\left(\frac{j\pi}{2}\right) \sin(nA) \right) \sin\left(\frac{j\pi}{2}\right) \\ &= \csc(2A) \sin^2\left(\frac{j\pi}{2}\right) \sin(nA) \\ &= \frac{1 - (-1)^j}{2} \csc(2A) \sin((2^{t+1}\ell + r)A) \\ &= \frac{1 - (-1)^j}{2} \csc(2A) (-1)^\ell \sin(rA). \end{aligned}$$

Certainly (with $k = 2^t + 2s + 1$),

$$\begin{aligned} wt(X(d, n)) &= \sum_{k \in J(d)} \sum_{i \equiv k \pmod{2^{t+1}}, i \leq n} C(n, i) \\ &\leq \sum_{k \in I(t)} A_n^{2^{t+1}}(k) = \sum_{s=0}^{2^{t-1}-1} A_n^{2^{t+1}}(2^t + 2s + 1). \end{aligned}$$

Then, using (19) and (20)

$$\begin{aligned} (21) \quad \sum_{s=0}^{2^{t-1}-1} A_n^{2^{t+1}}(2^t + 2s + 1) &= 2^{n-2} + 2^{n-t} \sum_{s=0}^{2^{t-1}-1} \sum_{j=1}^{2^t-1} (-1)^j (\cos A)^n \cos((n-2-4s)A) \\ &= 2^{n-2} + 2^{n-t} \sum_{j=1}^{2^t-1} (-1)^j (\cos A)^n \sum_{s=0}^{2^{t-1}-1} \cos((n-2-4s)A) \\ &= 2^{n-2} + 2^{n-t} \sum_{j=1}^{2^t-1} (-1)^{\ell+j} (\cos A)^n \frac{1 - (-1)^j \frac{\sin(rA)}{\sin(2A)}}{2} \\ &= 2^{n-2} + 2^{-t} (-1)^{\ell+1} \sum_{j=1, \text{ odd}}^{2^t-1} (2 \cos A)^{n-1} \frac{\sin(rA)}{\sin A} := S \end{aligned}$$

But the last sum is strictly positive by Lemmas 19 and 20. Therefore, if ℓ is even, $S < 2^{n-2}$, and this proves our lemma. \square

Remark 4. We see that if $n = 2^{t+1}\ell + r$, ℓ odd and $r < 2^t$, then we can write $n = 2^{t+1}\ell + r = 2^{t+1}(\ell - 1) + 2^{t+1} + r$, with $\ell - 1$ even, and $0 \leq r' := 2^{t+1} + r < 2^{t+1} + 2^t$. Thus, the only cases left unchecked in the previous lemma (which gives many cases of Conjecture 1) are: $n = 2^{t+1}\ell + r$, ℓ odd, $2^t \leq r < 2^{t+1}$.

6. THE CASE $wt(d) \geq 3$

Lemma 9, Corollary 3 and Lemma 20 show that Conjecture 1 holds for any $X(d, n)$ with $d = 2^t$. A key fact, given in the proof of Lemma 20, is a useful formula for $wt(X(d, n))$ when $wt(d) = 2$. We can find a similar formula when $wt(d) = 3$, however it becomes substantially harder to handle.

Lemma 22. Let $d := 1 + 2^s + 2^t$, where $1 \leq s < t$ and $t \geq 2$. Then

$$\begin{aligned} (22) \quad wt(X(d, n)) &= 2^{n-3} - 2^{-t} \sum_{j=1, \text{ odd}}^{2^t-1} (2 \cos A)^{n-1} \frac{\sin((n-2^s)A) \sin(2^s A)}{\sin A \sin(2^{s+1} A)} \\ &\quad - 2^{-s-1} \sum_{k=1, \text{ odd}}^{2^s-1} (2 \cos B)^{n-1} \frac{\sin(nB)}{\sin B} \end{aligned}$$

Proof. Let $A = \frac{j\pi}{2^{t+1}}$, $B = \frac{k\pi}{2^{s+1}}$. From $d \preceq i$, we get that $i = 2^{t+1}i' + 2^t + 2^{s+1}p + 2^s + 2q + 1$, and so, $i \equiv 2^t + 2^{s+1}p + 2^s + 2q + 1 \pmod{2^{t+1}}$. Certainly the converse

is also true. Using the previous observation,

(23)

$$\begin{aligned}
wt(X(d, n)) &= \sum_{d \preceq i \leq n} C(n, i) = \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} A_n^{2^{t+1}} (2^t + 2^{s+1}p + 2^s + 2q + 1) \\
&= \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} \left(2^{n-t-1} + 2^{-t} \sum_{j=1}^{2^t-1} (2 \cos A)^n \cos((n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 4q - 2)A) \right) \\
&= 2^{t-s-1} 2^{s-1} 2^{n-t-1} + 2^{-t} \sum_{j=1}^{2^t-1} (2 \cos A)^n \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} \cos((n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 4q - 2)A) \\
&= 2^{n-3} + 2^{-t} \sum_{j=1}^{2^t-1} (2 \cos A)^n \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} \cos((n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 4q - 2)A)
\end{aligned}$$

using Lemma 18. Further, by using formula (17) with $x = -4A$, $y = (n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 2)A$, $N = 2^{s-1} - 1$, the innermost sum is equal to

$$\begin{aligned}
&\csc(x/2) \cos(Nx/2 + y) \sin((N+1)x/2) \\
&= \csc(-2A) \cos((2^{s-1} - 1)(-2A) + (n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 2)A) \sin(2^{s-1}(-2A)) \\
&= \csc(2A) \cos((n - 2^{t+1} - 2^{s+2}p - 3 \cdot 2^s)A) \sin(2^s A),
\end{aligned}$$

which is defined everywhere, since $j \leq 2^t - 1$. Thus,

(24)

$$wt(X(d, n)) = 2^{n-3} + 2^{-t} \sum_{j=1}^{2^t-1} (2 \cos A)^{n-1} \frac{\sin(2^s A)}{\sin A} \sum_{p=0}^{2^{t-s-1}-1} \cos((n - 2^{t+1} - 2^{s+2}p - 3 \cdot 2^s)A).$$

Let

$$U := \{j : j = 2^{t-s}k, 1 \leq k \leq 2^s - 1\}$$

We distinguish two cases:

Case 1. Assume $j \in U$. That means that

$$2^{s+2}A = 2^{s+2} \frac{j\pi}{2^{t+1}} = 2^{s+2} \frac{k2^{t-s}\pi}{2^{t+1}} = 2k\pi,$$

and using the periodicity of the cosine function, we obtain that in this case, the innermost sum is

$$2^{t-s-1} \cos((n - 2^{t+1} - 3 \cdot 2^s)A).$$

Case 2. Assume $j \notin U$. In this case, we apply again formula (17) with $x = -2^{s+1}A$, $y = (n - 2^{t+1} - 3 \cdot 2^s)A$, $N = 2^{t-s-1} - 1$, the innermost sum is equal to

$$\begin{aligned}
&\csc(-2^{s+1}A) \cos((2^{t-s-1} - 1)(-2^{s+1}A) + (n - 2^{t+1} - 3 \cdot 2^s)A) \sin(2^{t-s-1}(-2^{s+1}A)) \\
&= \csc(2^{s+1}A) \cos(-2^t A + (n - 2^{t+1} - 2^s)A) \sin(2^t A) \\
&= \csc(2^{s+1}A) \cos((n - 2^s)A - 3j\pi/2) \sin(j\pi/2) \\
&= \csc(2^{s+1}A) \cos((n - 2^s)A + j\pi/2) \sin(j\pi/2)
\end{aligned}$$

Thus, from equation (24), we obtain (note that $A = B$, if $j = 2^{t-s}k$; also, $2^{t+1}A = j\pi$, $2^sB = k\pi/2$)

(25)

$$\begin{aligned}
wt(X(d, n)) &= 2^{n-3} + 2^{-t} \sum_{j=1, j \notin U}^{2^t-1} (2 \cos A)^{n-1} \frac{\cos((n-2^s)A + j\pi/2) \sin(j\pi/2) \sin(2^s A)}{\sin A \sin(2^{s+1} A)} \\
&\quad + 2^{-t} \sum_{j=1, j \in U}^{2^t-1} (2 \cos A)^{n-1} \frac{\sin(2^s A)}{\sin A} 2^{t-s-1} \cos((n-3 \cdot 2^s)A - j\pi) \\
&= 2^{n-3} + 2^{-t} \sum_{j=1, j \notin U}^{2^t-1} (2 \cos A)^{n-1} \frac{\cos((n-2^s)A + j\pi/2) \sin(j\pi/2) \sin(2^s A)}{\sin A \sin(2^{s+1} A)} \\
&\quad + 2^{-s-1} \sum_{k=1}^{2^s-1} (2 \cos B)^{n-1} \frac{\sin(k\pi/2)}{\sin B} \cos((n-3 \cdot 2^s)B - 2^{t-s}k\pi) \\
&= 2^{n-3} + 2^{-t} \sum_{j=1, j \notin U}^{2^t-1} (2 \cos A)^{n-1} \frac{\cos((n-2^s)A + j\pi/2) \sin(j\pi/2) \sin(2^s A)}{\sin A \sin(2^{s+1} A)} \\
&\quad + 2^{-s-1} \sum_{k=1}^{2^s-1} (2 \cos B)^{n-1} \frac{\sin(k\pi/2)}{\sin B} \cos(nB + k\pi/2).
\end{aligned}$$

(The last equality follows from the periodicity of \cos , and also from $\cos((n-3 \cdot 2^s)B) = \cos(nB - 3k\pi/2) = \cos(nB + k\pi/2)$.) Further, if $j \notin U$, then $\sin(2^{s+1}A)$ is well defined, however $\sin(j\pi/2) = 0$, if j is even. Thus, the terms in the first sum of the last equation of (25) are zero, unless j is odd. Then, if j is odd, we get

$$\begin{aligned}
&\cos((n-2^s)A + j\pi/2) \sin(j\pi/2) \\
&= (\cos((n-2^s)A) \cos(j\pi/2) - \sin((n-2^s)A) \sin(j\pi/2)) \sin(j\pi/2) \\
&= -\sin((n-2^s)A).
\end{aligned}$$

Therefore,

$$\begin{aligned}
wt(X(d, n)) &= 2^{n-3} - 2^{-t} \sum_{j=1, \text{odd}}^{2^t-1} (2 \cos A)^{n-1} \frac{\sin((n-2^s)A) \sin(2^s A)}{\sin A \sin(2^{s+1} A)} \\
&\quad + 2^{-s-1} \sum_{k=1}^{2^s-1} (2 \cos B)^{n-1} \frac{\sin(k\pi/2)}{\sin B} \cos(nB + k\pi/2)
\end{aligned}$$

or better, yet,

$$\begin{aligned}
wt(X(d, n)) &= 2^{n-3} - 2^{-t} \sum_{j=1, \text{odd}}^{2^t-1} (2 \cos A)^{n-1} \frac{\sin((n-2^s)A) \sin(2^s A)}{\sin A \sin(2^{s+1} A)} \\
&\quad - 2^{-s-1} \sum_{k=1, \text{odd}}^{2^s-1} (2 \cos B)^{n-1} \frac{\sin(nB)}{\sin B}
\end{aligned}$$

□

In order to prove Conjecture 1, by Lemma 9 and Corollary 3 it would suffice to show that for $n \geq 2(d-1)$ (we can assume this because of Theorem 3) we have

$$(26) \quad wt(X(d, n)) \neq 2^{n-2}$$

for all pairs d, n except $d = 2^t + 1, n = 2^{t+1}\ell$, where t and ℓ are any positive integers.

Lemma 20 proves (26) when $wt(d) = 2$. We attempted to prove (26) when $wt(d) = 3$ by using Lemma 22, but the sums in (22) were too complicated to allow us to cover all of the cases. Certainly (22) shows that for fixed d , (26) holds for all sufficiently large n , because the factors $(\cos A)^{n-1}$ and $(\cos B)^{n-1}$ tend to 0 as $n \rightarrow \infty$, which implies $wt(X(d, n)) - 2^{n-2} < 0$ for all large n . Our computations suggest that this inequality will always hold if $wt(d)$ is large enough. In fact, we conjecture

Conjecture 2. If $n \geq 2(d-1)$, d is fixed and $wt(d) \geq 6$, then $wt(X(d, n)) - 2^{n-2} < 0$.

Acknowledgements. The authors would like to thank Prof. Jingbo Xia for the proof of Lemma 19, which simplified their original argument.

REFERENCES

- [1] A. Canteaut and M. Videau, “Symmetric Boolean Functions”, *IEEE Trans. on Information Theory* 51 (2005), 2791–2811.
- [2] C. Carlet, “On cryptographic propagation criteria for Boolean functions”, *Inform. and Comput.* 151 (1999), 32–56.
- [3] C. Carlet, “On the Degree, Nonlinearity, Algebraic Thickness, and Nonlinearity of Boolean Functions, With Development of Symmetric Functions”, *IEEE Trans. on Information Theory* 50 (2004), 2178–2185.
- [4] C.A. Charalambides, “Enumerative Combinatorics”, New York, *CRC Press*, 2002.
- [5] Chuan-kun Wu and Ed Dawson, “Correlation Immunity and Resiliency of Symmetric Boolean Functions”, *Theoretical Computer Science* 312 (2004), 321–335.
- [6] T.W. Cusick and Yuan Li “ k -th Order Symmetric SAC Boolean Functions and Bisecting Binomial Coefficients”, *Discrete Applied Mathematics* 149 (2005), 73–86.
- [7] Ed Dawson and Chuan-kun Wu, “On the Linear Structure of Symmetric Boolean Functions”, *Australasian Journal of Combinatorics* 16 (1997), 239–243.
- [8] Keqin Feng and Fengmei Liu, “New Results On The Nonexistence of Generalized Bent Functions”, *IEEE Trans. on Information Theory* 49 (2003), 3066–3071.
- [9] K. Gopalakrishnan, D.G. Hoffman and D.R. Stinson, “A Note on a Conjecture Concerning Symmetric Resilient Functions”, *Information Processing Letters* 47 (1993), 139–143.
- [10] J. von zur Gathen and J. Roche, “Polynomials with two values”, *Combinatorica* 17, no. 3 (1997), 345–362.
- [11] E.R. Hansen, “A Table of Series and Products”, (Prentice-Hall, Englewood Cliffs, NJ, 1975).
- [12] V. E. Hoggatt Jr. and G. L. Alexanderson, “Sums of partition sets in generalized Pascal triangles I”, *Fibonacci Quarterly* 14 (1976), 117–125.
- [13] J.M. Holte, “Asymptotic prime-power divisibility of binomial, generalized binomial, and multinomial coefficients”, *Trans. Amer. Math. Soc.* 349 (1997), no. 10, 3837–3873.
- [14] P.V. Kumar, R.A. Scholtz, and L.R. Welch, “Generalized Bent Functions and Their Properties”, *J. Combinatorial Theory (A)* 40 (1985), 90–107.
- [15] T. Lengyel, “On the order of lacunary sums of binomial coefficients”, *Integers* 3 (2003), A3, 10 pp.
- [16] Mulan Liu, Peizhong Lu and G.L. Mullen, “Correlation-Immune Functions over Finite Fields”, *IEEE Trans. on Information Theory* 44 (1998), 1273–1276.
- [17] F. J. MacWilliams and N. J. A. Sloane, “The Theory of Error-Correcting Codes” (Amsterdam: North Holland, 1978).
- [18] S. Maitra and P. Sarkar, “Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables”, *IEEE Trans. on Information Theory* 48 (2002), 2626–2630.
- [19] C. Mitchell, “Enumerating Boolean Functions of Cryptographic Significance”, *Journal of Cryptology* 2 (1990), 155–170.

- [20] P. Sarkar and S. Maitra, “Balancedness and Correlation Immunity of Symmetric Boolean Functions”, *Proceedings of the R.C. Bose Centenary Symposium, Electronic Notes in Discrete Mathematics*, 15 (2003), 178–183.
- [21] P. Savicky, “On the Bent Boolean Functions That Are Symmetric”, *Europ. J. Comb.* 15 (1994), 407–410.
- [22] P. Stănică, “Chromos, Boolean Functions and Avalanche Characteristics”, Ph.D. Thesis, State University of New York at Buffalo, 1998.
- [23] Yuan Li and T.W. Cusick, “Strict Avalanche Criterion over Finite Fields”, submitted, 2005.
- [24] Yuan Li and T.W. Cusick, “Linear Structures of Symmetric Functions over Finite Fields”, *Information Processing Letters* 97 (2006), 124–127.
- [25] Yupu Hu and Guozhen Xiao “Resilient Functions Over Finite Fields”, *IEEE Trans. on Information Theory* 49 (2003), 2040–2046.
- [26] Y.X. Yang and B. Guo, “Futher Enumerating Boolean Functions of Cryptographic Significance”, *Journal of Cryptology* 8 (3), 1995, 115–122.

¹SUNY, DEPARTMENT OF MATHEMATICS, 244 MATHEMATICS BUILDING, BUFFALO, NY 14260
E-mail address: email: `cusick@buffalo.edu`

²DEPARTMENT OF MATHEMATICAL SCIENCES, ALCORN STATE UNIVERSITY, ALCORN STATE, MS 39096
E-mail address: email: `yuanli7983@gmail.com`

³APPLIED MATHEMATICS DEPARTMENT, NAVAL POSTGRADUATE SCHOOL, MONTEREY, CA 93943
E-mail address: email: `pstanica@nps.edu`